SESSIONS

# Data Processing Addendum

This Data Processing Addendum, including its Exhibits (this “**Addendum**” or ”**DPA”**) , forms part of the Terms and Conditions or any other agreement about the delivery of the contracted services (the “**Agreement**”) between Sessions Technologies Inc and its Affiliates (“**Sessions**”) and the specific customer entity engaging in the Agreement ("Customer" or ”End User”) to reflect the parties' agreement about the Processing of Customer Personal Data (as those terms are defined below).

## 1. Definitions

1.1. “Affiliate” means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party. For purposes of this DPA, “control” means an economic or voting interest of at least fifty percent 50% or, in the absence of such economic or voting interest, the power to direct or cause the direction of the management and set the policies of such an entity.

1.2. "Biometric Data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;

1.3. "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

1.4. “Customer Personal Data” means Personal Data, including but not limited to:

1.4.1. Content Data: All text, sound, video, or files that are part of an Customers’ profile and information exchanged between Customers (including guest users participating in Customer-hosted meetings or workspace members) and with Sessions via the Services;

1.4.2. Account Data (name, screen name and email address);

1.4.3. Biometric Data (vocal recording and video recording);

1.4.4. Website access Data (including cookies);

1.4.5. Diagnostic Data, including but not limited to: Data from applications (including browsers) installed on End User devices, Service generated server logs (for example meeting metadata and End User settings) and internal security logs that are generated by or provided to Sessions;

1.5. "Personal Data" means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.6. "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

1.7. “Services” means the Sessions Services as set forth in the terms and conditions of the Agreement ("T&C") available here.

## 2. Processing Activities

2.1. Both parties hereby acknowledge and consent to the stipulations outlined below: The Customer assumes the position of Controller concerning the handling of Customer Personal Data. Sessions, on the other hand, functions as the Processor for Customer Personal Data, unless Sessions or an affiliated entity assumes the role of Controller, engaging in the processing of Customer Personal Data solely for legitimate business purposes.

2.2. In consideration of necessity and proportionality, the Customer, in its capacity as the Controller, issues directives to Sessions to execute the subsequent activities as the Processor on behalf of the Customer:

2.2.1. The provisioning and continual updates of the Services, configured and utilized by the Customer and its users, encompassing adjustments made through the Customer's manipulation of Sessions' settings or administrator controls. These adjustments aim at continuous product enhancement and the delivery of personalized experiences and recommendations;

2.2.2. Ensuring the security and real-time monitoring of the Services;

2.2.3. Addressing issues, bugs, and errors;

2.2.4. Providing support at the request of the Customer, incorporating insights derived from individual customer support requests for the collective benefit of all Sessions customers, with the proviso that such insights are limited to anonymized knowledge;

2.2.5. Processing Customer Personal Data in line with the terms specified in the T&C, covering the subject matter, nature, purpose, and duration of Personal Data Processing in the capacity of a processor, in response to documented instructions provided by the Customer and acknowledged by Sessions as constituting instructions under this DPA, collectively referred to as the "Instructions."

2.3. The Customer affirms and guarantees that (i) it has adhered to, and will consistently adhere to, all pertinent laws, including data protection laws, concerning the processing of Customer Data and any processing directives issued to Sessions; and (ii) it has furnished, and will persist in furnishing, all requisite notices, and has secured, and will persist in securing, all consents and rights mandated by data protection laws to enable Sessions to process Customer Data for the purposes delineated in the T&C. The Customer bears exclusive responsibility for the precision, quality, and legality of Customer Data, as well as the methodologies employed in acquiring such data. Without diminishing the scope of the above, the Customer agrees to assume responsibility for compliance with all applicable laws (inclusive of data protection laws) pertinent to any content created, dispatched, or managed through the Service. This includes obligations related to obtaining consents, where necessary, for video or voice recording and the content of recordings.

2.4. The Customer will ensure that Sessions' processing of Customer Data, in accordance with the Customer's instructions, does not lead to Sessions violating any applicable laws, regulations, or rules, including, but not limited to, data protection laws. Sessions will promptly inform the Customer in writing, unless prevented by European Data Protection Laws, if it becomes aware or believes that any data processing directive from the Customer contravenes European data protection laws. In instances where the Customer acts as a processor on behalf of a third-party controller (or another intermediary to the ultimate controller), the Customer affirms that its processing directives, as outlined in the T&C and this DPA, including its authorizations to Sessions for the appointment of sub-processors as per this DPA ("Sub-processors "), have received authorization from the relevant controller. The Customer will serve as the exclusive point of contact for Sessions, and Sessions is not obliged to engage directly with (including providing notifications to or seeking authorization from) any third-party controller, except through the regular provision of the Service as required under the T&C. The Customer will be responsible for forwarding any notifications received under this DPA to the relevant controller, where applicable.

## 3. Sub-processing

3.1. The Customer acknowledges that Sessions may enlist the services of Sub-processors to handle Customer Data on behalf of the Customer. You can find the updated list of Sub-processors engaged by Sessions in the Sessions Privacy Policy page or in a similar page made public by Sessions.

3.2. Obligations of Sub-Processors. Sessions shall: (i) establish a written agreement with each Sub-processor that includes data protection obligations ensuring a level of protection for Customer Data equivalent to the provisions in this DPA, to the extent applicable to the nature of the service provided by each Sub-processor; and (ii) retain responsibility for the Sub-processor's adherence to the obligations set forth in this DPA, as well as for any actions or oversights by the Sub-processor that result in Sessions breaching its obligations under this DPA. Sessions may be restricted from disclosing Sub-processor agreements to the Customer due to confidentiality constraints, but upon request, Sessions shall make reasonable efforts to provide the Customer with all pertinent information within its reasonable capacity in connection with Sub-processor agreements.

## 4. Security

4.1. *Implementation of Security Measures*. Sessions shall establish and uphold suitable technical and organizational security measures crafted to safeguard Customer Data against Security Incidents. These measures are designed to maintain the security and confidentiality of Customer Data in accordance with Sessions' security standards delineated in Schedule 1 ("Security Measures") of this DPA.

4.2. *Confidentiality in Processing*. Sessions shall ensure that any individual authorized by Sessions to process Customer Data, including its personnel, agents, and subcontractors, is bound by a fitting obligation of confidentiality, whether contractual or statutory in nature.

4.3. *Updates to Security Measures*. The Customer is tasked with assessing the information provided by Sessions concerning data security and independently determining whether the Service aligns with the Customer's requirements and legal obligations under Data Protection Laws. The Customer acknowledges that the Security Measures may undergo technical advancements and modifications over time, and Sessions may periodically update or modify them, provided such updates and modifications do not compromise the overall security of the Service provided to the Customer.

4.4. *Response to Security Incidents*. In the event of a Security Incident coming to Sessions' attention, Sessions shall: (i) promptly notify the Customer, where feasible, within 48 hours of awareness; (ii) furnish timely information related to the Security Incident as it becomes known or as reasonably requested by the Customer; and (iii) expeditiously take reasonable measures to contain and investigate any Security Incident. It is important to note that Sessions' notification or response to a Security Incident, as outlined in this Section 4.4, does not imply acknowledgment of any fault or liability on the part of Sessions regarding the Security Incident.

4.5. *Customer Responsibilities*. Despite the aforementioned, the Customer agrees that, except as stipulated in this DPA, it holds responsibility for the secure usage of the Service. This includes safeguarding account authentication credentials, ensuring the security of Customer Data during transit to and from the Service, and taking necessary measures to securely encrypt or back up any Customer Data uploaded to the Service.

## 5. Data Transfers

5.1. Unless otherwise stipulated in Section 5 of the DPA, the Customer acknowledges that Sessions may transfer and process Customer Data in the United States and globally, wherever Sessions, its Affiliates, or its Sub-processors conduct data processing operations. Sessions shall consistently ensure that these transfers comply with the requirements set forth in data protection laws and this DPA.

## 6. Data Retention

6.1. Upon the termination or expiration of the Agreement, Sessions shall, at the Customer's choice, either delete or return all Customer Data (including copies) within its possession or control. This requirement excludes instances where applicable law mandates the retention of some or all Customer Data, or for Customer Data archived on backup systems. In such cases, Sessions shall securely isolate and protect the archived Customer Data from further processing and eventually delete it in alignment with Sessions' deletion policies, except to the extent required by applicable law.

## 7. Data Subject Rights and Cooperation

7.1. Considering the nature of the processing, Sessions shall provide reasonable assistance to the Customer to the extent possible, enabling compliance with data protection obligations related to data subject rights under data protection Laws. If a Data Subject request is directly made to Sessions, Sessions shall not respond to such communication unless authorized by the Customer or legally required. In cases where Sessions is mandated to respond, and the Customer is identifiable from the request, Sessions shall promptly notify the Customer and provide a copy of the request, unless legally prohibited.

## 8. Data Protection Impact Assessment.

8.1. As required by applicable data protection laws, Sessions shall provide all reasonably requested information regarding the Service to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities. Sessions shall comply with this obligation and, if necessary, offering additional reasonable assistance upon request, at the Customer's expense.

## 9. Jurisdiction-Specific Terms

9.1. In the event of any conflict or ambiguity between the jurisdiction-specific terms and other terms of this DPA, the applicable jurisdiction-specific terms will take precedence, but only to the extent of their applicability to Sessions.

## 10. Limitation of Liability

10.1. The aggregate liability of each party and its Affiliates arising from or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the T&C.

10.2. Claims against Sessions or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

10.3. In no event shall any party limit its liability concerning any individual's data protection rights under this DPA or otherwise.

## 11. Relationship with the Agreement

11.1. This DPA remains effective as long as Sessions carries out Customer Data processing operations on behalf of the Customer or until the termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 6 above).

11.2. This DPA replaces any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service.

11.3. In case of conflict or inconsistency between this DPA and the T&C, the following documents, in order of precedence, shall prevail: (i) this DPA; and (ii) the T&C.

11.4. Except for changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5. Only a party to this DPA, its successors, and permitted assignees have the right to enforce any of its terms.

11.6. This DPA is governed by and constructed in accordance with the governing law and jurisdiction provisions in the T&C, unless required otherwise by applicable data protection laws.

**[SIGNATURE PAGE FOLLOWS]**

**THE COMPANY:**

SESSIONS TECHNOLOGIES, INC.

By:

DocuSigned by:

Radu Negulescu

9567849BD893464...

______________________

(Signature)

Name: Radu Negulescu

Title: CEO and Director

Date: 12 February 2024

---

**CUSTOMER**

______________________

By:

______________________

(Signature)

Name: ______________________

Title: ______________________

Date: ______________________

## Schedule 1

## Security Measures

Sessions places a strong emphasis on data security and privacy, acknowledging the significance of our security measures and practices to you. While we are cautious about disclosing intricate details, which might compromise our protective efforts, we can share general information to assure you of our commitment to safeguarding the data you place in our trust.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

We implement industry-standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignments, and traditional firewall rules.

Static code analysis: Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development, and research, troubleshoot potential problems, detect and respond to security incidents, and implement data security. Administrative or high-risk access permissions are reviewed at least once every six months.

Background checks: All Sessions employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces. Our HTTPS implementation uses industry-standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.0% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation, and air conditioning (HVAC) services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure.

Online backups: All databases are backed up and maintained using at least industry standard methods.

Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure the availability of information following interruption to, or failure of, critical business processes.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.